CLAIMS

WHAT IS CLAIMED IS:

1. A memory management unit for managing a memory storing data arranged within a plurality of memory pages, the memory management unit comprising:

a security check unit coupled to receive a physical address within a selected memory page and security attributes of the selected memory page, and wherein the security check unit is configured to use the physical address to access at least one security attribute data structure located in the memory to obtain an additional security attribute of the selected memory page, and to generate a fault signal dependent upon the security attributes of selected memory page and the additional security attribute of the selected memory page.

2. The memory management unit as recited in claim 1, wherein the security attributes of the selected memory page comprise a user/supervisor (U/S) bit and a read/write (R/W) bit as defined by the x86 processor architecture, and wherein U/S=0 indicates the selected memory page is an operating system memory page and corresponds to a supervisor level of the operating system, and wherein U/S=1 indicates the selected memory page is a user memory page and corresponds to a user level of the operating system, and wherein R/W=0 indicates only read accesses are allowed to the selected memory page, and wherein R/W=1 indicates that both read and write accesses are allowed to the selected memory page.

3. The memory management unit as recited in claim 1, wherein the at least one security attribute data structure comprises a security attribute table directory and at least one security attribute table.

4. The memory management unit as recited in claim 3, wherein the security attribute table directory comprises a plurality of entries, and where each entry of the security attribute table directory includes a present bit and a security attribute table base address field, and wherein the present bit indicates whether or not a security attribute table corresponding to the security attribute table directory entry is present in the memory, and wherein the security attribute table base address field is reserved for a base address of the security attribute table corresponding to the security attribute table directory entry.

5. The memory management unit as recited in claim 3, wherein the at least one security attribute table comprises a plurality of entries, and where each entry of the security attribute table includes a secure page (SP) bit, and wherein the SP bit indicates whether or not a corresponding memory page is a secure page.

6. The memory management unit as recited in claim 1, wherein the additional security attribute of the selected memory page comprises a secure page (SP) bit, and wherein the SP bit indicates whether or not the selected memory page is a secure page.

7. The memory management unit as recited in claim 1, wherein the linear address is produced during execution of an instruction residing within a first memory page, and wherein the security check unit is coupled to receive a current privilege level (CPL) of a task including the instruction, and wherein the security check logic is configured obtain an additional security attribute of the first memory page from the at least one security attribute data structure, and wherein the security check logic is configured to generate the fault signal dependent upon the CPL of the task including the instruction, the additional security attribute

of the first memory page, the security attributes of the selected memory page, and the additional security attribute of the selected memory page.

8. The memory management unit as recited in claim 7, wherein the additional security attribute of the first memory page comprises a secure page (SP) bit, and wherein the SP bit indicates whether or not the first memory page is a secure page.

9. The memory management unit as recited in claim 1, wherein the linear address is produced during execution of an instruction residing within a first memory page, and wherein the security check unit is coupled to receive a value of a secure execution mode (SEM) bit indicative of operation in a secure execution mode, and wherein the security check logic is configured obtain an additional security attribute of the first memory page from the at least one security attribute data structure, and wherein the security check logic is configured to generate the fault signal dependent upon the value of the SEM bit, the additional security attribute of the first memory page, the security attributes of the selected memory page, and the additional security attribute of the selected memory page.

10. The memory management unit as recited in claim 1, wherein the fault signal is a page fault signal as defined by the x86 processor architecture.

11. A central processing unit, comprising:

an execution unit operably coupled to a memory, wherein the execution unit is configured to fetch instructions from the memory and to execute the instructions; and

a memory management unit (MMU) operably coupled to the memory and configured to manage the memory, wherein the MMU is configurable to manage the memory such that the memory stores data arranged within a plurality of memory pages, and wherein the MMU comprises:

a security check unit coupled to receive a physical address within a selected memory page and security attributes of the selected memory page, and wherein the security check unit is configured to use the physical address to access at least one security attribute data structure located in the memory to obtain an additional security attribute of the selected memory page, and to generate a fault signal dependent upon the security attributes of selected memory page and the additional security attribute of the selected memory page.

12. A computer system, comprising:

a memory for storing data, wherein the data includes instructions;

a central processing unit (CPU), comprising:

an execution unit operably coupled to the memory, wherein the execution unit is configured to fetch instructions from the memory and to execute the instructions; and

a memory management unit (MMU) operably coupled to the memory and configured to manage the memory, wherein the MMU is configurable to manage the memory such that the memory stores the data arranged within a plurality of memory pages, and wherein the MMU comprises:

a security check unit coupled to receive a physical address within a selected memory page and security attributes of the selected memory page, and wherein the security check unit is configured to use the physical address to access at least one security attribute data structure located in the memory to obtain an additional security attribute of the selected memory page, and to generate a fault signal dependent upon the security attributes of selected memory page and the additional security attribute of the selected memory page.

13. A memory management unit for managing a memory storing data arranged within a plurality of memory pages, the memory management unit comprising:

a paging unit coupled to the memory and to receive a linear address and configured to use the linear address to produce a physical address within a selected memory page, wherein the paging unit is configured use the linear address to access at least one paged memory data structure located in the memory to obtain security attributes of the selected memory page, and wherein the paging unit is configured to produce a fault signal dependent upon the security attributes of the selected memory page; and

wherein the paging unit comprises a security check unit coupled to receive the physical address and the security attributes of the selected memory page, and wherein the security check unit is configured to use the physical address of the selected memory page to access at least one security attribute data structure located in the memory to obtain an additional security attribute of the selected memory page, and to generate the fault signal dependent upon the security attributes of selected memory page and the additional security attribute of the selected memory page.

14. The memory management unit as recited in claim 13, wherein the paging unit produces the physical address of the selected memory page during execution of an instruction residing within a first memory page.

15. The memory management unit as recited in claim 13, wherein the physical address within the selected memory page includes a base address and an offset.

16. The memory management unit as recited in claim 15, wherein the paging unit is configured to obtain the base address from the at least one paged memory data structure.

17. The memory management unit as recited in claim 13, wherein the at least one paged memory data structure comprises a page directory and at least one page table as defined by the x86 processor architecture.

18. The memory management unit as recited in claim 13, wherein the security attributes of the selected memory page comprise a user/supervisor (U/S) bit and a read/write (R/W) bit as defined by the x86 processor architecture, and wherein U/S=0 indicates the selected memory page is an operating system memory page and corresponds to a supervisor level of the operating system, and wherein U/S=1 indicates the selected memory page is a user memory page and corresponds to a user level of the operating system, and wherein R/W=0 indicates only read accesses are allowed to the selected memory page, and wherein R/W=1 indicates that both read and write accesses are allowed to the selected memory page.

19. The memory management unit as recited in claim 14, wherein the paging unit is configured to receive security attribute of the instruction and to produce the fault signal dependent upon the security attribute of the instruction and the security attributes of the selected memory page.

20. The memory management unit as recited in claim 19, wherein the security attribute of the instruction comprises a current privilege level (CPL) of a task including the instruction as defined by the x86 processor architecture.

21. The memory management unit as recited in claim 19, wherein the security attribute of the instruction comprises a value of a secure execution mode (SEM) bit indicative of operation in a secure execution mode.

22. The memory management unit as recited in claim 13, wherein the at least one security attribute data structure comprises a security attribute table directory and at least one security attribute table.

23. The memory management unit as recited in claim 22, wherein the security attribute table directory comprises a plurality of entries, and where each entry of the security attribute table directory includes a present bit and a security attribute table base address field, and wherein the present bit indicates whether or not a security attribute table corresponding to the security attribute table directory entry is present in the memory, and wherein the security attribute table base address field is reserved for a base address of the security attribute table corresponding to the security attribute table directory entry.

24. The memory management unit as recited in claim 22, wherein the at least one security attribute table comprises a plurality of entries, and where each entry of the security attribute table includes a secure page (SP) bit, and wherein the SP bit indicates whether or not a corresponding memory page is a secure page.

25. The memory management unit as recited in claim 24, wherein the additional security attribute of the selected memory page comprises a secure page (SP) bit, and wherein the SP bit indicates whether or not the selected memory page is a secure page.

26. The memory management unit as recited in claim 20, wherein the security check unit is coupled to receive the CPL of the task including the instruction, and wherein the security check logic is configured obtain an additional security attribute of the first memory page including the instruction from the at least one security attribute data structure, and wherein the security check logic is configured to generate the fault signal dependent upon the CPL of the task including the instruction, the additional security attribute of the first memory page

including the instruction, the security attributes of the selected memory page, and the additional security attribute of the selected memory page.

27. The memory management unit as recited in claim 26, wherein the additional security attribute of the first memory page comprises a secure page (SP) bit, and wherein the SP bit indicates whether or not the first memory page is a secure page.

28. The memory management unit as recited in claim 21, wherein the security check unit is coupled to receive the value of the SEM bit, and wherein the security check logic is configured obtain an additional security attribute of the first memory page including the instruction from the at least one security attribute data structure, and wherein the security check logic is configured to generate the fault signal dependent upon the value of the SEM bit, the additional security attribute of the first memory page including the instruction, the security attributes of the selected memory page, and the additional security attribute of the selected memory page.

29. The memory management unit as recited in claim 13, wherein the fault signal is a page fault signal as defined by the x86 processor architecture.

30. A memory management unit for managing a memory storing data arranged within a plurality of memory pages, the memory management unit comprising:

a paging unit coupled to the memory and to receive a linear address produced during execution of an instruction residing within a first memory page, wherein the paging unit is configured to use the linear address to produce a physical

address accessed by the instruction, and wherein the physical address includes a base address of a selected memory page and an offset, and wherein the paging unit is configured to access at least one paged memory data structure located in the memory using the linear address to obtain the base address and security attributes of the selected memory page, and wherein the paging unit is configured to receive security attribute of the instruction, and wherein the paging unit is configured to produce a fault signal dependent upon the security attribute of the instruction and the security attributes of the selected memory page; and

wherein the paging unit comprises a security check unit coupled to receive the security attribute of the instruction, the security attributes of the selected memory page, and the physical address within the selected memory page, and wherein the security check unit is configured to access at least one security attribute data structure located in the memory using the physical address of the selected memory page to obtain an additional security attribute of the first memory page and an additional security attribute of the selected memory page, and to generate the fault signal dependent upon the security attribute of the instruction, the additional security attribute of the first memory page, the security attributes of the selected memory page, and the additional security attribute of the selected memory page.

31. The memory management unit as recited in claim 30, wherein the at least one paged memory data structure comprises a page directory and at least one page table as defined by the x86 processor architecture.

32. The memory management unit as recited in claim 30, wherein the security attribute of the instruction comprises a current privilege level (CPL) of a task including the instruction as defined by the x86 processor architecture.

33. The memory management unit as recited in claim 30, wherein the security attribute of the instruction comprises a value of a secure execution mode (SEM) bit indicative of operation in a secure execution mode.

34. The memory management unit as recited in claim 30, wherein the security attributes of the selected memory page comprise a user/supervisor (U/S) bit a read/write (R/W) bit as defined by the x86 processor architecture, and wherein U/S=0 indicates the selected memory page is an operating system memory page and corresponds to a supervisor level of the operating system, and wherein U/S=1 indicates the selected memory page is a user memory page and corresponds to a user level of the operating system, and wherein R/W=0 indicates only read accesses are allowed to the selected memory page, and wherein R/W=1 indicates that both read and write accesses are allowed to the selected memory page.

35. The memory management unit as recited in claim 30, wherein the fault signal is a page fault signal as defined by the x86 processor architecture.

36. The memory management unit as recited in claim 30, wherein the additional security attribute of the first memory page comprises a secure page (SP) bit, and wherein the SP bit indicates whether or not the first memory page is a secure page.

37. The memory management unit as recited in claim 30, wherein the additional security attribute of the selected memory page comprises a secure page (SP) bit, and wherein the SP bit indicates whether or not the selected memory page is a secure page.

38. The memory management unit as recited in claim 30, wherein the at least one security attribute data structure comprises a security attribute table directory and at least one security attribute table.

39. The memory management unit as recited in claim 38, wherein the security attribute table directory comprises a plurality of entries, and where each entry of the security attribute table directory includes a present bit and a security attribute table base address field, and wherein the present bit indicates whether or not a security attribute table corresponding to the security attribute table directory entry is present in the memory, and wherein the security attribute table base address field is reserved for a base address of the security attribute table corresponding to the security attribute table directory entry.

40. The memory management unit as recited in claim 38, wherein the at least one security attribute table comprises a plurality of entries, and where each entry of the security attribute table includes a secure page (SP) bit, and wherein the SP bit indicates whether or not a corresponding memory page is a secure page.

41. A method for providing access security for a memory used to store data arranged within a plurality of memory pages, the method comprising:

receiving a linear address produced during execution of an instruction and a security attribute of the instruction, wherein the instruction resides in a first memory page;

using the linear address to access at least one paged memory data structure located in the memory to obtain a base address of a selected memory page and security attributes of the selected memory page;

combining the base address of the selected memory page with an offset to produce a physical address within the selected memory page if the security attribute of the instruction and the security attributes of the selected memory page indicate the access is authorized;

generating a fault signal if the security attribute of the instruction and the security attributes of the selected memory page indicate the access is not authorized;

accessing at least one security attribute data structure located in the memory using the physical address of the selected memory page to obtain an additional security attribute of the first memory page and an additional security attribute of the selected memory page; and

generating the fault signal dependent upon the security attribute of the instruction, the additional security attribute of the first memory page, the security attributes of the selected memory page, and the additional security attribute of the selected memory page.

42. The method as recited in claim 41, wherein the using comprises:

using the linear address to access at least one paged memory data structure located in the memory to obtain a base address of a selected memory page and security attributes of the selected memory page, wherein the at least one paged memory data structure comprises a page directory and at least one page table as defined by the x86 processor architecture.

43. The method as recited in claim 41, wherein the receiving comprises:

receiving a linear address produced during execution of an instruction and a security attribute of the instruction, wherein the instruction resides in a first memory page, and wherein the security attribute of the instruction comprises a current privilege level (CPL) of a task including the instruction as defined by the x86 processor architecture.

44. The method as recited in claim 41, wherein the receiving comprises:

receiving a linear address produced during execution of an instruction and a security attribute of the instruction, wherein the instruction resides in a first memory page, and wherein the security attribute of the instruction comprises a value of a secure execution mode (SEM) bit indicative of operation in a secure execution mode.

45. The method as recited in claim 41, wherein the using comprises:

using the linear address to access at least one paged memory data structure located in the memory to obtain a base address of a selected memory page and security attributes of the selected memory page, wherein the security attributes of the selected memory page comprise a user/supervisor (U/S) bit a read/write (R/W) bit as defined by the x86 processor architecture, and wherein U/S=0 indicates the selected memory page is an operating system memory page and corresponds to a supervisor level of the operating system, and wherein U/S=1 indicates the selected memory page is a user memory page and corresponds to a user level of the operating system, and wherein R/W=0 indicates only read accesses are allowed to the selected memory page, and wherein R/W=1 indicates that both read and write accesses are allowed to the selected memory page.

46. The method as recited in claim 41, wherein the generating comprises:

generating the fault signal dependent upon the security attribute of the instruction, the additional security attribute of the first memory page, the security attributes of the selected memory page, and the additional security attribute of the selected memory page, wherein the fault signal is a page fault signal as defined by the x86 processor architecture.

47. The method as recited in claim 41, wherein the accessing comprises:

accessing at least one security attribute data structure located in the memory using the physical address of the selected memory page to obtain an additional security attribute of the first memory page and an additional security attribute of the selected memory page, wherein the additional security attribute of the first memory page comprises a secure page (SP) bit, and wherein the SP bit indicates whether or not the first memory page is a secure page.

48. The method as recited in claim 41, wherein the accessing comprises:

accessing at least one security attribute data structure located in the memory using the physical address of the selected memory page to obtain an additional security attribute of the first memory page and an additional security attribute of the selected memory page, wherein the additional security attribute of the selected memory page comprises a secure page (SP) bit, and wherein the SP bit indicates whether or not the selected memory page is a secure page.

49. The method as recited in claim 41, wherein the using comprises:

using the linear address to access at least one paged memory data structure located in the memory to obtain a base address of a selected memory page and security attributes of the selected memory page, wherein the at least one security attribute data structure comprises a security attribute table directory and at least one security attribute table.